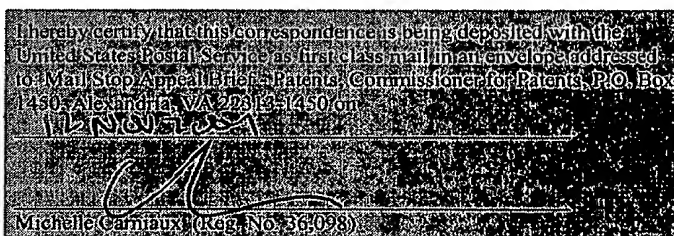


IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BOARD OF PATENT APPEALS AND INTERFERENCES

-----X
 In re Application of: David N. FELDMAN et al. : Examiner: C. Sherr
 :
 :
 For: SYSTEMS AND METHODS FOR :
 SERVERLESS SOFTWARE LICENSING :
 : Art Unit: 3621
 :
 Filed: March 29, 2000 :
 :
 Serial No.: 09/537,086 :
 -----X

Mail Stop Appeal Brief - Patents
 Commissioner for Patents
 P.O. Box 1450
 Alexandria, VA 22313-1450



APPEAL BRIEF TRANSMITTAL

SIR:

Transmitted herewith for filing in the above-identified patent application please find an Appeal Brief pursuant to 37 C.F.R. § 41.37.

Please charge the Appeal Brief fee of \$340.00, and any other fees that may be required in connection with this communication to the deposit account of **Kenyon & Kenyon**, deposit account number **11-0600**. A duplicate of this paper is attached for this purpose.

Appellants hereby request a five-month extension of time for submitting the Appeal Brief. The extended period for submitting the Appeal Brief expires on November 12, 2004. Please charge the \$2,080.00 extension fee and any other fee that may be required to Deposit Account No. 11-0600. A duplicate of this Transmittal is enclosed

Dated: 12 Nov 2004


Respectfully submitted,

By: 
 Michelle Carniaux
 Registration No. 36,098

KENYON & KENYON
 One Broadway
 New York, NY 10004
 (212) 425-7200
CUSTOMER NO. 26646

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BOARD OF PATENT APPEALS AND INTERFERENCES

-----X	
In re Application of:	:
David N. FELDMAN et al.	:
	:
For:	:
SYSTEMS AND METHODS FOR	:
SERVERLESS SOFTWARE LICENSING	:
	:
Filed:	:
March 29, 2000	:
Serial No.: 09/537,086	:

I hereby certify that this correspondence is being deposited with the	
United States Postal Service with sufficient postage as first class mail	
in an envelope addressed to:	
Mail Stop <u>Appeal - Patents</u>	
Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450	
on	
Mail Stop Appeal Brief - Patents	Date <u>12 Nov 2004</u>
Commissioner for Patents	Atty's Reg. # <u>36,098</u>
P.O. Box 1450	Atty's Signature <u></u>
Alexandria, VA 22313-1450	MICHELLE M. CARNIAUX
	KENYON & KENYON

APPEAL BRIEF PURSUANT TO 37 C.F.R. § 41.37(a)(1)

On April 12, 2004, the U.S. Patent Office received Appellants' Notice of Appeal (mailed April 9, 2004) from the final rejection of claims 1-97 contained in the Final Office Action issued by the U.S. Patent and Trademark Office on October 9, 2003 in the above-identified patent application.

In accordance with 37 C.F.R. § 41.37(a), this brief is submitted in support of the appeal of the final rejection of claims 1-97. For at least the reasons set forth below, the final rejection of claims 1-97 should be reversed.

(i). REAL PARTY IN INTEREST

The real party in interest in the present appeal is Viewpoint Corporation, New York, NY. Metastream Corporation is the assignee of the entire right, title and interest in the present application. The previous assignee, Viewpoint Corporation, was previously doing business as Metastream Corporation and is the successor in interest to the present application.

Concurrently, documentation is being prepared for filing with the U.S. Patent Office in the present application to update the assignee of record.

(ii). RELATED APPEALS AND INTERFERENCES

There are no interferences or other appeals related to the present application.

(iii). STATUS OF CLAIMS

Claims 1-97 current stand rejected under 35 U.S.C. §102(e) as being anticipated by U.S. Patent No. 6,502,079 (hereinafter referred to as the "Ball patent").

Appellants appeal from the final rejection of claims 1-97. A copy of all of the pending claims is attached hereto in the Appendix.

(iv). STATUS OF AMENDMENTS

No amendments are currently outstanding.

(v). SUMMARY OF THE CLAIMED SUBJECT MATTER

As noted in the specification, with some software applications, problems arise in the proper detecting and accounting for use-based licensing. Therefore, the present invention provides for serverless software licensing. The present claimed subject matter includes, *inter alia*, independent claims 1, 15, 27, 34, 39, 44, 60, 74, 81, 88 and 90.

Claim 1 recites a method for controlling the use of a data object using encrypted network address information including, *inter alia*, receiving a data object and encrypted network address information from a server, such as illustrated in step 200 of Fig. 2. A computer 106 of Fig. 1 running a plug-in software application receives the content data object and the encrypted address information from the server 101. The computer 106 executing the plug-in software may thereupon play the contents of the data object, such as

illustrated in step 210 of Fig. 2. Also, the encrypted address information is decrypted, such as in one embodiment using a public key, as illustrated in step 220 of Fig. 2. In one embodiment, the present invention further includes, *inter alia*, determining if the decrypted network address information corresponds to a network address of the server, such as illustrated in step 230 of Fig. 2. This may be accomplished by any suitable means, such as comparing the network address of the server with the decrypted network address. In one embodiment, if the decrypted network address information does not correspond to the network address, the contents of the data object cease being played, such as illustrated in step 250 of Fig. 2.

Claim 15 recites a method for controlling the playing of content using encrypted network address information including, *inter alia*, receiving a data object and network address information from a first server, similar to step 500 of Fig. 5. A computer 106 of Fig. 1 running a plug-in software application receives the content data object and the address information from the server 101. The computer 106 executing the plug-in software may thereupon play the contents of the data object, such as illustrated in step 510 of Fig. 5. Also, the encrypted address information is decrypted, such as in one embodiment using a public key, as illustrated in step 520 of Fig. 5. In one embodiment, the present invention further includes, *inter alia*, receiving a plurality of network addresses from a second server corresponding to decrypted network address information, such as illustrated in step 550 of Fig. 5. In one embodiment, a search is conducted of the plurality of network addresses for a network address of the first server, such as illustrated in step 560 of Fig. 5. In this embodiment, if the decrypted network address information does not correspond to the network address, the contents of the data object cease being played, such as illustrated in step 570 of Fig. 5.

Claim 27 recites a method for controlling the playing of content using encrypted network address information including, *inter alia*, receiving a data object and network address information from a server, similar to step 500 of Fig. 5. A computer 106 of Fig. 1 running a plug-in software application receives the content data object and the address information from the server 101. The computer 106 executing the plug-in software may thereupon play the contents of the data object, such as illustrated in step 510 of Fig. 5. Also, the encrypted address information is decrypted, such as in one embodiment using a public key, as illustrated in step 520 of Fig. 5. In one embodiment, a search is conducted

of the plurality of network addresses for a network address of the first server, such as illustrated in step 560 of Fig. 5. In this embodiment, if the search fails, the contents of the data object cease being played, such as illustrated in step 570 of Fig. 5.

Claim 34 recites a method for calculating license fees for client software based on the network address of the content provider including, *inter alia*, receiving a plurality of records from a plurality of software clients wherein each record includes a network address, such as illustrated in step 800 of Fig. 8. In one embodiment, the method includes determining the number of records that include a particular network address, such as illustrated in step 810 of Fig. 8, and calculating a license fee the particular network address based on the number of records, such as illustrated in step 820 of Fig. 8.

Claim 39 recites a system for calculating software license fees including, *inter alia*, software clients, such as clients 106 of Fig. 1, content servers, such as server 101 of Fig. 1 and a billing server, such as server 104 of Fig. 1. Similar to the method of claim 34 and as illustrated generally in Fig. 8, in this system, the software clients download and play content from the content servers, log information about the content played, and send the logged information to the billing server. In one embodiment, the billing server uses the logged information from the software clients to calculate the number of times that content from each content server was played. The billing server then uses the number of times to calculate a license fee to be charged to the entity that operates the content server.

Claim 44 recites a method for controlling the playing of content using encrypted network address information including, *inter alia*, receiving a data object and network address information from a server, similar to step 300 of Fig. 3. A computer 106 of Fig. 1 running a plug-in software application receives the content data object and the address information from the server 101. The encrypted address information is decrypted, such as in one embodiment using a public key, as illustrated in step 310 of Fig. 3. In one embodiment, a determination is made whether the decrypted network address information corresponds to a network address of the server, such as illustrated in step 320 of Fig. 3. In this embodiment, if the correspondence exists, the contents of the data object are played, such as illustrated in step 330 of Fig. 3.

Claim 60 recites an article of manufacture including a computer readable medium having instructions stored thereon. These instructions are adapted to be executed by a processor. The instructions, when executed, define a series of steps to be used to control

the playing of the contents of a data object. The steps include, *inter alia*, receiving a data object and network address information from a server, similar to step 300 of Fig. 3. The encrypted network address information is decrypted, such as in one embodiment using a public key, as illustrated in step 310 of Fig. 3. In one embodiment, a determination is made whether the decrypted network address information corresponds to a network address of the server, such as illustrated in step 320 of Fig. 3. In this embodiment, if the correspondence exists, the contents of the data object are played, such as illustrated in step 330 of Fig. 3.

Claim 74 recites an article of manufacture including a computer readable medium having instructions stored thereon. These instructions are adapted to be executed by a processor. The instructions, when executed, define a series of steps to be used to control the playing of the contents of a data object. The steps include, *inter alia*, receiving a data object and network address information from a server, similar to step 500 of Fig. 5. A computer 106 of Fig. 1 running a plug-in software application receives the content data object and the address information from the server 101. The computer 106 executing the plug-in software may thereupon play the contents of the data object, such as illustrated in step 510 of Fig. 5. Also, the encrypted address information is decrypted, such as in one embodiment using a public key, as illustrated in step 520 of Fig. 5. In one embodiment, a search is conducted of the plurality of network addresses for a network address of the first server, such as illustrated in step 560 of Fig. 5. In this embodiment, if the search fails, the invention ceases playing the contents of the data object, such as illustrated in step 570 of Fig. 5.

Claim 81 recites an article of manufacture including a computer readable medium having instructions stored thereon. These instructions are adapted to be executed by a processor. The instructions, when executed, define a series of steps to be used to control the playing of the contents of a data object. The steps include, *inter alia*, receiving a data object and network address information from a first server, similar to step 500 of Fig. 5. A computer 106 of Fig. 1 running a plug-in software application receives the content data object and the address information from the server 101. The computer 106 executing the plug-in software may thereupon play the contents of the data object, such as illustrated in step 510 of Fig. 5. Also, the encrypted address information is decrypted, such as in one embodiment using a public key, as illustrated in step 520 of Fig. 5. In one embodiment,

the present invention further includes, *inter alia*, receiving a plurality of network addresses from a second server corresponding to decrypted network address information, such as illustrated in step 550 of Fig. 5. In one embodiment, a search is conducted of the plurality of network addresses for a network address of the first server, such as illustrated in step 560 of Fig. 5. In this embodiment, if the decrypted network address information does not correspond to the network address, contents of the data object cease to be played, such as illustrated in step 570 of Fig. 5.

Claim 88 recites an article of manufacture including a computer readable medium having instructions stored thereon. These instructions are adapted to be executed by a processor. The instructions, when executed, define a series of steps to calculate license fees for client software based on the network address of the content provider. The steps include, *inter alia*, receiving a plurality of records from a plurality of software clients wherein each record includes a network address, such as illustrated in step 800 of Fig. 8. In one embodiment, the method includes determining the number of records that include a particular network address, such as illustrated in step 810 of Fig. 8, and calculating a license fee the particular network address based on the number of records, such as illustrated in step 820 of Fig. 8.

Claim 90 recites a method for controlling the use of a data object using network address information including, *inter alia*, receiving a data object and network address information from a server, similar to step 200 of Fig. 2. A computer 106 of Fig. 1 running a plug-in software application receives the content data object and the address information from the server 101. The computer 106 executing the plug-in software may thereupon play the contents of the data object, such as illustrated in step 210 of Fig. 2. Also, a message is sent to a verification server containing the network address information. In one embodiment, the present invention further includes, *inter alia*, receiving a response from the verification server and ceasing to play the contents of the data object if the response from the verification server is negative.

(vi). **GROUND OF REJECTION TO BE REVIEWED ON APPEAL**

Whether claims 1-97, which stand rejected under 35 U.S.C. §102(e), are patentable over the Ball patent.

(vii). **ARGUMENTS**

Claims 1-97 stand rejected under 35 U.S.C. §102(e) as being anticipated by the Ball patent. It is respectfully submitted that the Ball patent does not anticipate any of claims 1-97 for at least the following reasons.

The Ball patent describes a floating license enforcement system. Ball describes a license management system for managing the leniency of a “floating” license using an earned credit mechanism. The system of Ball utilizes “credit tokens” which a user accumulates during licensed use of a software application, the tokens are accumulated according to an accumulation rate (Ar). If a license fault occurs, Ball describes consuming these accumulated tokens at two possible token consumption rates based on user activity. If a user utilizes the software application, the tokens are consumed according to an extinct consumption rate. If the user does not utilize the software application, the tokens are consumed according to a graced consumption rate. Once all the tokens are consumed and if the license fault is not resolved, the licensed application is terminated. The Ball system tracks the number of tokens (which represent credit for units of time) in case of a software license fault, only explicitly denying software execution upon consumption of ALL token. In the Ball system, the tokens are internally controlled, as well as maintaining usage of the tokens. In other words, Ball distinctly describes a system for compensating when an licensed application is unable to access and confirm a license agreement from a vendor.

In order for a claim to be anticipated under 35 U.S.C. § 102, a single prior art reference must disclose each and every element of the claim in exactly the same way. *See Lindeman Maschinenfabrik v. Am. Hoist and Derrick*, 730 F.2d 1452, 1458 (Fed. Cir. 1984); MPEP § 2131. Appellants respectfully submit that this criteria for establishing anticipation is not met here.

Claims 1-14, 44-59, and claims 60-73

Claim 1 recites the following:

A method for controlling the use of a data object using encrypted network address information, comprising the steps of:

receiving a data object and encrypted network address information from a server;
playing the contents of said data object;
decrypting said encrypted network address information;
determining whether said decrypted network address

information corresponds to a network address of said server; and

if said correspondence does not exist, ceasing to play the contents of said data object.

Claim 44 recites the following:

A method for controlling the playing of content using encrypted network address information, comprising the steps of:

receiving a data object and encrypted network address information from a server;

decrypting said encrypted network address information;

determining whether said decrypted network address information corresponds to a network address of said server; and

if said correspondence does exist, playing the contents of said data object.

Claim 60 recites the following:

An article of manufacture comprising a computer-readable medium having stored thereon instructions adapted to be executed by a processor, the instructions which, when executed, define a series of steps to be used to control the playing of the contents of a data object, said steps comprising:

receiving a data object and encrypted network address information from a server;

decrypting said encrypted network address information;

determining whether said decrypted network address information corresponds to a network address of said server; and

if said correspondence exists, playing the contents of said data object.

Respectfully, Ball does not describe “receiving a data object and encrypted network address information from a server,” “decrypting said encrypted network address information” or “determining whether said decrypted network address information corresponds to a network address of said server.”

As compared to the Ball patent, certain embodiments of the present application, for example, use encrypted network address information to control a data object received from a server. Once received, the encrypted network address information is decrypted and

compared to the address of the server from which it was received. If the address information does not match, use of the data object is not allowed or is only allowed in a limited form. Ball does not describe using encrypted network address information to control the use of data objects, rather as noted above, Ball describes a self-controlled token accounting system to control software execution. In other words Ball describes a completely different system using tokens, to generate a complete different result which is the internal monitoring of the time of usage of a licensed application and produces a completely different result including disabling execution of the application when the tokens are consumed prior to resolution of a license fault.

Claims 2 to 14, 43 to 59 and 61 to 73 depend from claims 1, 44 and 60. Accordingly, the arguments presented above in connection with claims 1, 44 and 60 apply equally to claims 2 to 14, 43 to 59 and 61 to 73. In view of the foregoing, it is submitted that Ball does not anticipate any of claims 1 to 14 or 44 to 73.

Claims 15-26 and 81-87

Claim 15 recites the following:

A method for controlling the playing of content using encrypted network address information, comprising the steps of:

receiving a data object and encrypted network address information from a first server;

playing the contents of said data object;

decrypting said encrypted network address information;

receiving a plurality of network addresses from a second server corresponding to said decrypted network address information;

searching said plurality of network addresses for a network address of said first server; and

if said search fails, ceasing to play the contents of said data object.

Claim 81 recites the following:

An article of manufacture comprising a computer-readable medium having stored thereon instructions adapted to be executed by a processor, the instructions which, when executed, define a series of steps to be used to control the playing of the contents of a data object, said steps comprising:

receiving a data object and encrypted network address information from a first server;

playing the contents of said data object;
*decrypting said encrypted network address
information;*
*receiving a plurality of network addresses from a
second server corresponding to said decrypted network
address information;*
*searching said plurality of network addresses for a
network address of said first server; and*
if said search fails, ceasing to play the contents of
said data object.

Respectfully, as explained above, Ball does not describe “receiving a data object and encrypted network address information from a first server” or “decrypting said encrypted network address information.” Furthermore, Ball does not describe “receiving a plurality of network addresses from a second server corresponding to said decrypted network address information” and “searching said plurality of network addresses for a network address of said first server.”

As compared with the Ball patent, certain embodiments of the present invention, for example, use encrypted network address information to control a data object received from a first server. Once received, the encrypted network address information is decrypted and a list of network addresses is received from a second server, the second server corresponding to the decrypted network address information. This list of network addresses is then compared to the address of the first server from which the data object was received. If the first server’s address information is not found in the list, use of the data object is not allowed or is only allowed in a limited form. Ball does not describe using encrypted network address information in this way to control the use of data objects, rather as noted above, Ball describes a self-controlled token accounting system to control software execution. In other words Ball describes a completely different system using tokens, to generate a complete different result which is the internal monitoring of the time of usage of a licensed application and produces a completely different result including disabling execution of the application when the tokens are consumed prior to resolution of a license fault.

Claims 16 to 26 and 82 to 87 depend from claims 15 and 81. Accordingly, the arguments presented above in connection with claims 15 and 81 apply equally to claims 16 to 26 and 82 to 87. In view of the foregoing, it is submitted that Ball does not anticipate any of claims 15 to 26 or 81 to 87.

Claims 27-33 and 75-80

Claim 27 recites the following:

A method for controlling the playing of content using encrypted network address information, comprising the steps of:

receiving a data object and encrypted network address information from a server;
playing the contents of said data object;
decrypting said encrypted network address information;
searching a plurality of network addresses for a network address corresponding to said decrypted network address information; and
if said search succeeds, ceasing to play the contents of said data object.

Claim 74 recites the following:

An article of manufacture comprising a computer-readable medium having stored thereon instructions adapted to be executed by a processor, the instructions which, when executed, define a series of steps to be used to control the playing of the contents of a data object, said steps comprising:

receiving a data object and encrypted network address information from a server;
playing the contents of said data object;
decrypting said encrypted network address information;
searching a plurality of network addresses for a network address corresponding to said decrypted network address information; and
if said search succeeds, ceasing to play the contents of said data object.

Respectfully, as explained above, Ball does not describe “receiving a data object and encrypted network address information from a server” or “decrypting said encrypted network address information.” Furthermore, Ball does not describe “searching a plurality of network addresses for a network address corresponding to said decrypted network address information.”

In contrast, certain embodiments of the present invention, for example, use encrypted network address information to control a data object received from a server. Once received, the encrypted network address information is decrypted and compared to a

list of network addresses. If the server's address information is found in the list, use of the data object is not allowed or is only allowed in a limited form. Ball does not describe using encrypted network address information in this way to control the use of data objects, rather as noted above, Ball describes a self-controlled token accounting system to control software execution. In other words Ball describes a completely different system using tokens, to generate a complete different result which is the internal monitoring of the time of usage of a licensed application and produces a completely different result including disabling execution of the application when the tokens are consumed prior to resolution of a license fault.

Claims 28 to 33 and 75 to 80 depend from claims 27 and 74. Accordingly, the arguments presented above in connection with claims 27 and 74 apply equally to claims 28 to 33 and 75 to 80. In view of the foregoing, it is submitted that Ball does not anticipate any of claims 27 to 33 or 74 to 80.

Claims 34-43 and 88-89

Claim 34 recites the following:

A method for calculating license fees for client software based on the network address of the content provider, comprising the steps of:

receiving a plurality of records from a plurality of software clients wherein each record includes a network address;

determining the number of records of said plurality of records that include a particular network address; and

calculating a license fee for said particular network address based on said number of records.

Claim 39 recites the following:

A system for calculating software licensing fees, comprising:

a plurality of software clients;

a plurality of content servers; and

a billing server,

wherein each of said plurality of software clients downloads and plays content from said plurality of content servers, *logs information about the content played, and sends said logged information to said billing server; and said billing server uses the logged information received from said plurality of software clients to calculate the number of times that content from each content server was*.

played and uses said number of times to calculate a license fee to be charged to the entity that operates the content server.

Claim 88 recites the following:

An article of manufacture comprising a computer-readable medium having stored thereon instructions adapted to be executed by a processor, the instructions which, when executed, define a series of steps to be used to calculate license fees for client software based on the network address of the content provider, said steps comprising:

receiving a plurality of records from a plurality of software clients wherein each record includes a network address;

*determining the number of records of said plurality of records that include a particular network address; and
calculating a license fee for said particular network address based on said number of records.*

Respectfully, Ball does not describe “receiving a plurality of records from a plurality of software clients wherein each record includes a network address,” “determining the number of records of said plurality of records that include a particular network address” or “calculating a license fee for said particular network address based on said number of records.” Nor does Ball describe software clients “log[ging] information about the content played, and send[ing] said logged information to said billing server” and a billing server “us[ing] the logged information received from said plurality of software clients to calculate the number of times that content from each content server was played and us[ing] said number of times to calculate a license fee to be charged to the entity that operates the content server.”

In contrast, in certain embodiments of the present invention, for example, software clients log information about content they have downloaded/played from a content server and send that information to a billing server. The billing server then uses this information to calculate how many times content from each content server was downloaded/played and calculates a corresponding license fee to be charged to the entity which operates the content server. This calculation may be made, for example, by counting the number of times the content server’s network address appears in the logged information. Ball does not describe using information logged by software clients and sent to a billing server to calculate licensing fees for content providers, rather as noted above, Ball describes a self-

controlled token accounting system to control software execution. In other words Ball describes a completely different system using tokens, to generate a complete different result which is the internal monitoring of the time of usage of a licensed application and produces a completely different result including disabling execution of the application when the tokens are consumed prior to resolution of a license fault..

Claims 35 to 38, 40 to 43 and 89 depend from claims 34, 39 and 88. Accordingly, the arguments presented above in connection with claims 34, 39 and 88 apply equally to claims 35 to 38, 40 to 43 and 89. In view of the foregoing, it is submitted that Ball does not anticipate any of claims 34 to 43, 88 or 89.

Claims 90-97

Claim 90 recites the following:

A method for controlling the use of a data object using network address information, comprising the steps of:
receiving a data object and network address information from a server;
playing the contents of said data object;
sending a message to a verification server containing said network address information;
receiving a response from said verification server;
and
if said response is negative, ceasing to play the contents of said data object.

Respectfully, Ball does not describe “receiving a data object and network address information from a server” and “sending a message to a verification server containing said network address information.”

In contrast, certain embodiments of the present invention control the use of data objects by, for example, sending a message to a verification server including network address information received with the data object, and awaiting a message from the verification server verifying that the network address information belongs to a licensed content provider. Ball does not describe using network address information and a message to a verification server to control the use of data objects, rather as noted above, Ball describes a self-controlled token accounting system to control software execution. In other words Ball describes a completely different system using tokens, to generate a complete different result which is the internal monitoring of the time of usage of a licensed application and produces a completely different result including disabling execution of the

application when the tokens are consumed prior to resolution of a license fault..

Claims 91 to 97 depend from claim 90. Accordingly, the arguments presented above in connection with claim 90 apply equally to claims 91 to 97. In view of the foregoing, it is submitted that Ball does not anticipate any of claims 90 to 97.

In view of the foregoing, it is respectfully submitted that the Ball patent does not anticipate any of claims 1-97. Reversal of the rejection of claims 1-97 is, therefore, requested.

CONCLUSION

For at least the reasons indicated above, Appellants respectfully submit that the art of record does not anticipate Appellants' invention as recited in the claims of the above-identified application. Accordingly, it is respectfully submitted that the invention recited in the claims of the present application is new, non-obvious and useful. Reversal of the Examiner's rejections of the claims is therefore respectfully requested.

Respectfully submitted,

Dated: 12 Nov 2004

By: 

Michelle Carniaux
Registration No. 36,098

KENYON & KENYON
One Broadway
New York, NY 10004
(212) 425-7200

APPENDIX

1. A method for controlling the use of a data object using encrypted network address information, comprising the steps of:
 - receiving a data object and encrypted network address information from a server;
 - playing the contents of said data object;
 - decrypting said encrypted network address information;
 - determining whether said decrypted network address information corresponds to a network address of said server; and
 - if said correspondence does not exist, ceasing to play the contents of said data object.
2. The method of claim 1 wherein said network address information is a Uniform Resource Locator.
3. The method of claim 1 wherein said network address information includes a domain name.
4. The method of claim 1 wherein said network address information includes a directory name.
5. The method of claim 1 wherein said network address information includes an Internet Protocol address.
6. The method of claim 1 wherein said decrypting step employs the public key of a public/private key pair to decrypt said encrypted network address information.
7. The method of claim 1 wherein said decrypting step employs a digital signature scheme to decrypt said encrypted network address information.
8. The method of claim 1 wherein said encrypted network address information is included in said data object.
9. The method of claim 1 wherein said encrypted network address information is included in a world wide web page residing on said server.
10. The method of claim 1 wherein the encrypted network address information also includes license information.
11. The method of claim 10 wherein the license information includes an expiration date.
12. The method of claim 1 further comprising the steps of:

- storing logging information about said data object; and
periodically sending said logging information to a remote network location.
- 13. The method of claim 12 wherein said logging information includes the network address information.
- 14. The method of claim 12 wherein said logging information includes information about the individual who requested the data object.
- 15. A method for controlling the playing of content using encrypted network address information, comprising the steps of:
 - receiving a data object and encrypted network address information from a first server;
 - playing the contents of said data object;
 - decrypting said encrypted network address information;
 - receiving a plurality of network addresses from a second server corresponding to said decrypted network address information;
 - searching said plurality of network addresses for a network address of said first server; and
 - if said search fails, ceasing to play the contents of said data object.
- 16. The method of claim 15 further comprising the steps of:
 - storing logging information about said data object; and
 - periodically sending said logging information to a third server.
- 17. The method of claim 16 wherein said logging information includes the network address information.
- 18. The method of claim 16 wherein said logging information includes information about the individual who requested the data object.
- 19. The method of claim 15 wherein said network address information is a Uniform Resource Locator.
- 20. The method of claim 15 wherein said network address information includes an Internet Protocol address.
- 21. The method of claim 15 wherein said decrypting step employs the public key of a public/private key pair to decrypt said encrypted network address information.
- 22. The method of claim 15 wherein said decrypting step employs a digital signature scheme to decrypt said encrypted network address information.

23. The method of claim 15 wherein said encrypted network address information is included in said data object;
24. The method of claim 15 wherein said encrypted network address information is included in a world wide web page residing on said server.
25. The method of claim 15 wherein the encrypted network address information also includes license information.
26. The method of claim 25 wherein the license information includes an expiration date.
27. A method for controlling the playing of content using encrypted network address information, comprising the steps of:
- receiving a data object and encrypted network address information from a server;
 - playing the contents of said data object;
 - decrypting said encrypted network address information;
 - searching a plurality of network addresses for a network address corresponding to said decrypted network address information; and
 - if said search succeeds, ceasing to play the contents of said data object.
28. The method of claim 27 wherein said network address information is a Uniform Resource Locator.
29. The method of claim 27 wherein said network address information includes an Internet Protocol address.
30. The method of claim 27 wherein said decrypting step employs the public key of a public/private key pair to decrypt said encrypted network address information.
31. The method of claim 27 wherein said decrypting step employs a digital signature scheme to decrypt said encrypted network address information.
32. The method of claim 27 wherein said encrypted network address information is included in said data object;
33. The method of claim 27 wherein said encrypted network address information is included in a world wide web page residing on said server.
34. A method for calculating license fees for client software based on the network address of the content provider, comprising the steps of:
- receiving a plurality of records from a plurality of software clients wherein each record includes a network address;

determining the number of records of said plurality of records that include a particular network address; and

calculating a license fee for said particular network address based on said number of records.

35. The method of claim 34 further comprising the step of:

selecting said particular network address from the plurality of network addresses included in said plurality of records.

36. The method of claim 35 further comprising the step of:

repeating said determining and said calculating steps until a license fee has been calculated for each unique network address that is included in said plurality of records.

37. The method of claim 36 wherein if said number of records that include said particular network address is less than a predesignated value, then the license fee is set to zero.

38. The method of claim 35 wherein if said number of records that include said particular network address is less than a predesignated value, then the license fee is set to zero.

39. A system for calculating software licensing fees, comprising:

a plurality of software clients;

a plurality of content servers; and

a billing server,

wherein each of said plurality of software clients downloads and plays content from said plurality of content servers, logs information about the content played, and sends said logged information to said billing server; and said billing server uses the logged information received from said plurality of software clients to calculate the number of times that content from each content server was played and uses said number of times to calculate a license fee to be charged to the entity that operates the content server.

40. The system of claim 39 wherein said logged information includes a network address for the content server from which the content was downloaded.

41. The system of claim 39 wherein said logged information includes information about the user of the client software.

42. The system of claim 39 wherein said client software verifies that the content server from which the content has been downloaded has agreed to a set of licensing terms.

43. The system of claim 42 wherein a public key encryption scheme is used by said client software to perform the verification.
44. A method for controlling the playing of content using encrypted network address information, comprising the steps of:
- receiving a data object and encrypted network address information from a server;
 - decrypting said encrypted network address information;
 - determining whether said decrypted network address information corresponds to a network address of said server; and
 - if said correspondence does exist, playing the contents of said data object.
45. The method of claim 44 further comprising the step of:
- if said correspondence does not exist, playing the contents of said data object in a diminished capacity.
46. The method of claim 44 further comprising the step of:
- if said correspondence does not exist, playing the contents of said data object with diminished quality.
47. The method of claim 44 further comprising the step of:
- if said correspondence does not exist, playing the contents of said data object with diminished functionality.
48. The method of claim 44 further comprising the steps of:
- storing logging information about said data object; and
 - periodically sending said logging information to a second server.
49. The method of claim 48 wherein said logging information includes the network address information.
50. The method of claim 48 wherein said logging information includes information about the individual who requested the data object.
51. The method of claim 45 further comprising the steps of:
- storing logging information about said data object; and
 - periodically sending said logging information to a second server.
52. The method of claim 51 wherein said logging information includes the network address information.
53. The method of claim 51 wherein said logging information includes information about the individual who requested the data object.

54. The method of claim 45 wherein said network address information is a Uniform Resource Locator.
55. The method of claim 45 wherein said network address information includes an Internet Protocol address.
56. The method of claim 45 wherein said decrypting step employs the public key of a public/private key pair to decrypt said encrypted network address information.
57. The method of claim 45 wherein said decrypting step employs a digital signature scheme to decrypt said encrypted network address information.
58. The method of claim 45 wherein said encrypted network address information is included in said data object.
59. The method of claim 45 wherein said encrypted network address information is included in a world wide web page residing on said server.
60. An article of manufacture comprising a computer-readable medium having stored thereon instructions adapted to be executed by a processor, the instructions which, when executed, define a series of steps to be used to control the playing of the contents of a data object, said steps comprising:
- receiving a data object and encrypted network address information from a server;
 - decrypting said encrypted network address information;
 - determining whether said decrypted network address information corresponds to a network address of said server; and
 - if said correspondence exists, playing the contents of said data object.
61. The article of manufacture of claim 60 further comprising the step of:
- if said correspondence does not exist, playing the contents of said data object with diminished quality.
62. The article of manufacture of claim 60 further comprising the step of:
- if said correspondence does not exist, playing the contents of said data object with diminished functionality.
63. The article of manufacture of claim 60 wherein said series of steps further comprise the steps of:
- storing logging information about said data object; and
 - periodically sending said logging information to a second server.
64. The article of manufacture of claim 63 wherein said logging information includes

the network address information.

65. The article of manufacture of claim 63 wherein said logging information includes information about the user of the article of manufacture.

66. The article of manufacture of claim 60 wherein said network address information is a Uniform Resource Locator.

67. The article of manufacture of claim 60 wherein said network address information includes an Internet Protocol address.

68. The article of manufacture of claim 60 wherein said decrypting step employs the public key of a public/private key pair to decrypt said encrypted network address information.

68. The article of manufacture of claim 60 wherein said decrypting step employs a digital signature scheme to decrypt said encrypted network address information.

70. The article of manufacture of claim 60 wherein said encrypted network address information is included in said data object.

71. The article of manufacture of claim 60 wherein said encrypted network address information is included in a world wide web page residing on said server.

72. The article of manufacture of claim 60 wherein the encrypted network address information also includes license information.

73. The article of manufacture of claim 72 wherein the license information includes an expiration date.

74. An article of manufacture comprising a computer-readable medium having stored thereon instructions adapted to be executed by a processor, the instructions which, when executed, define a series of steps to be used to control the playing of the contents of a data object, said steps comprising:

receiving a data object and encrypted network address information from a server;

playing the contents of said data object;

decrypting said encrypted network address information;

searching a plurality of network addresses for a network address corresponding to said decrypted network address information; and

if said search succeeds, ceasing to play the contents of said data object.

75. The article of manufacture of claim 74 wherein said network address information is a Uniform Resource Locator.

76. The article of manufacture of claim 74 wherein said network address information includes an Internet Protocol address.
77. The article of manufacture of claim 74 wherein said decrypting step employs the public key of a public/private key pair to decrypt said encrypted network address information.
78. The article of manufacture of claim 74 wherein said decrypting step employs a digital signature scheme to decrypt said encrypted network address information.
79. The article of manufacture of claim 74 wherein said encrypted network address information is included in said data object.
80. The article of manufacture of claim 74 wherein said encrypted network address information is included in a world wide web page residing on said server.
81. An article of manufacture comprising a computer-readable medium having stored thereon instructions adapted to be executed by a processor, the instructions which, when executed, define a series of steps to be used to control the playing of the contents of a data object, said steps comprising:
- receiving a data object and encrypted network address information from a first server;
 - playing the contents of said data object;
 - decrypting said encrypted network address information;
 - receiving a plurality of network addresses from a second server corresponding to said decrypted network address information;
 - searching said plurality of network addresses for a network address of said first server; and
 - if said search fails, ceasing to play the contents of said data object.
82. The article of manufacture of claim 81 wherein said network address information is a Uniform Resource Locator.
83. The article of manufacture of claim 81 wherein said network address information includes an Internet Protocol address.
84. The article of manufacture of claim 81 wherein said decrypting step employs the public key of a public/private key pair to decrypt said encrypted network address information.
85. The article of manufacture of claim 81 wherein said decrypting step employs a

digital signature scheme to decrypt said encrypted network address information.

86. The article of manufacture of claim 81 wherein said encrypted network address information is included in said data object.

87. The article of manufacture of claim 81 wherein said encrypted network address information is included in a world wide web page residing on said server.

88. An article of manufacture comprising a computer-readable medium having stored thereon instructions adapted to be executed by a processor, the instructions which, when executed, define a series of steps to be used to calculate license fees for client software based on the network address of the content provider, said steps comprising:

receiving a plurality of records from a plurality of software clients wherein each record includes a network address;

determining the number of records of said plurality of records that include a particular network address; and

calculating a license fee for said particular network address based on said number of records.

89. The article of manufacture of claim 88, wherein said series of steps further comprise the steps of:

selecting said particular network address from the plurality of network addresses included in said plurality of records; and

repeating said determining and said calculating steps until a license fee has been calculated for each unique network address that is included in said plurality of records.

90. A method for controlling the use of a data object using network address information, comprising the steps of:

receiving a data object and network address information from a server;

playing the contents of said data object;

sending a message to a verification server containing said network address information;

receiving a response from said verification server; and

if said response is negative, ceasing to play the contents of said data object.

91. The method of claim 90 wherein said network address information is a Uniform Resource Locator.

92. The method of claim 90 wherein said network address information includes a

domain name.

93. The method of claim 90 wherein said network address information includes a directory name.

94. The method of claim 90 wherein said network address information includes an Internet Protocol address.

95. The method of claim 90 further comprising the steps of:
storing logging information about said data object; and
periodically sending said logging information to a remote network location.

96. The method of claim 95 wherein said logging information includes the network address information.

97. The method of claim 95 wherein said logging information includes information about the individual who requested the data object.